Christopher Kirkpatrick, Secretary   Chris Barnard
Commodity Futures Trading Commission   Germany
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581
United States
www.cftc.gov

28 March 2024

- 17 CFR Parts 1, 23
- RIN Number 3038-AF23
- Operational Resilience Framework for Futures Commission Merchants,
  Swap Dealers, and Major Swap Participants

Dear Mr. Kirkpatrick.

Thank you very much for giving us the opportunity to comment on your notice of proposed rulemaking on Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants.

The Commodity Futures Trading Commission (CFTC) is proposing to require that futures commission merchants (FCMs), swap dealers (SDs), and major swap participants (MSPs) establish, document, implement, and maintain an Operational Resilience Framework (ORF) reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions to normal business operations. The framework would include three components – an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan – supported by broad requirements relating to governance, training, testing, and recordkeeping. The proposed rule would also require certain notifications to the CFTC and customers or counterparties. The CFTC is further proposing guidance relating to the management of risks stemming from third-party relationships.

I broadly support the CFTC's proposals, which are designed to accommodate entities of varying scale, scope and complexity and varying business models. The proposals will

promote sound risk management practices and strengthen the operational resilience of covered entities, protect market participants and the public from operational failures, enhance the financial integrity of derivatives markets, and reduce systemic risk within the financial system.

I would like now to provide some first, quick comments on the proposals. I support the following as key foundations and principles of an effective operational resilience framework (ORF) for covered entities:

- There must be a shift in emphasis from information security to operational risk and resilience management
- An effective ORF should require a consideration of risks across several activities and initiatives (dependencies) and their interaction with each other
- There should be no specification regarding materiality thresholds and no materiality limiter
- Source code from third parties and proprietary software must be checked for risks, vulnerabilities and anomalies in future

It is important that an effective ORF should place a strong focus on the internal governance regime and control environment of covered entities. It should also provide for detailed requirements for the board of directors and senior management and highlight and strengthen their role in the governance and control context.

Yours sincerely

C.R.B.

Chris Barnard